Bristol Village Computer Club
May, 2010

If you are reading this on your computer display, remember that **Acrobat Reader** has a ***zoom*** feature for enlarging text and graphics.

Computer Club (BVCC) Meeting, May 10, 2010, 7:30 PM

The meeting this month will feature: annual election of officers, business wrap up, ***What's up with Google?***, a review of popular web sites, and the usual question and answer session.

Notes from Kent

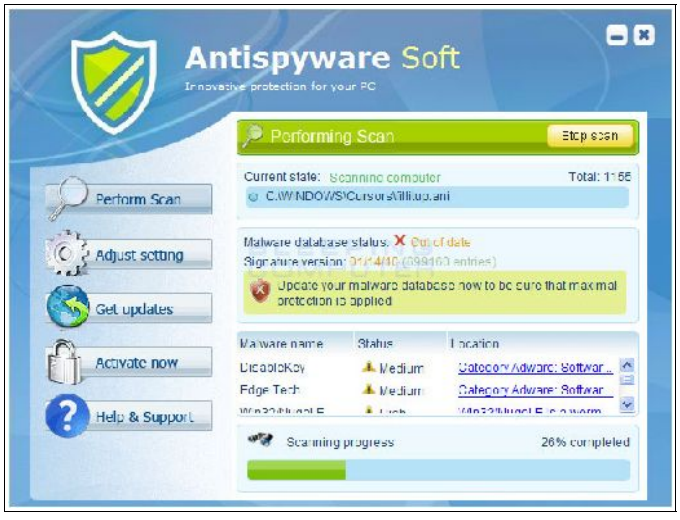
Ransomware

Two days ago, I had never heard of ***ransomware*** and now, as a result of helping Village residents, I have become too familiar with it. First, an explanation. ***Ransomware*** is a form of ***malware*** (derivation: "mal" meaning bad and "ware" meaning stuff; a generic term to cover viruses, Trojan horses, worms, and other things that interfere with your computer usage).

As its name implies, ransomware is a form of software that takes control of your data, its programs, and/or its operations and demands payment to return to you your own property. **Wickipedia**, **<http://en.wikipedia.org/wiki/Ransomware>,** offers an alternate definition: ***extortive*** malware. Still other security experts lump ransomware in a category ***scareware***, since its purpose is to scare you into sending money.

The ransomware close cousins (since they share many common graphics) encountered are ***antispyware soft*** and XP guardian. This latter seems to have about 66 variations and a list of these reads like a rap sheet for an habitual criminal, with akas (aka=also known as) such as ***antivirus XP, antivirus XP 2010, antispyware Vista***, and ***Win 7 Guardian***. ***Antispyware soft*** and ***XP guardian*** are trojan horses, that is, they pretend to be something beneficial while they are anything but. As evident in their names, these cousins claim that they are defenses against ***spyware***, viruses, and other malware when in fact they are the enemy they claim to oppose.

In operation, both programs generate pop-up warnings that your computer is infected, sometimes claiming with it is infected with thousands of viruses. They are right that it is infected but they are the infection. The following is a sample screen from ***antispyware soft***.



BVCC OFFICERS

President: Kent Mulliner
Vice President.: Don Netzley
Treasurer: George Hartwell
Secretary: Thurlie Knapp
Newsletter Editor: Len Nasman
CLUB EMAIL: bvclub@bvres.org

More to come, turn page ☞ ☞ ☞

Similarly, pop-up windows may resemble ordinary Window's pop-ups. The following is an example (common to both) of a more sophisticated warning that may be issued.

> **Antivirus software alert**
> Infiltration Alert
> Your computer is being attacked by an internet virus. It could be a password-stealing attack, a trojan - dropper or similar.
> **Details**
> Attack from: IP Address, port 39096
> Attacked Port: 30516
> Threat: Win32/Nuqel.E

The pervasive theme is that you should pay to protect your machine, data, or programs by activating its ***antivirus*** program. I confess that I'm not sure how payments are handled as one walks softly in dealing with an infection. One would think that the payment would be a trail leading to the offender, but I've heard of no arrests.

The most useful information that I found on these two programs was at http://www.bleepingcomputer.-com (one of the residents whose computer was infected assured me that more than '*bleeping*' was used in trying to use her infected computer). This site offers detailed removal instructions (after free registration) for each program. In the case of ***anti-spyware soft*** (http://www.bleepingcomputer.com/virus-removal/remove-antispyware-soft), it was necessary to change a setting so the computer does not use a proxy (a ransomware tactic to limit access to resources), start in **SAFE mode with a network connection** and then download a program **rkill** which suppressed the ransomware. All of this is followed by a free program Malwarebytes Antimalware (MBAM) which cleans out the system. For "XP Guardian" (http://www.bleepingcomputer.com/virus-removal/remove-antivirus-vista-2010), it was necessary to download to a flash drive a reg.fix program (which removes the ransomware's control of your system registration) before using MBAM.

To this point, I've failed to emphasize how disruptive either of these programs is. It essentially takes over control of your computer, denying access to programs, and even denying access to the internet (supposedly because the needed software is infected). ***Antispyware soft*** even went so far as to generate screens for full-screen ads for ***porn.com*** and ***viagra.com***. In fact, these malware are especially adept at protecting themselves (requiring the elaborate removal approaches above).

Malware is somewhat like cancer; it would be presumptuous to declare success in combating it. With this caveat in mind, the approaches described above seem to have been successful in restoring normal computer operations for the residents.

But even as we hope to have combated known instances of this ransomware, bleepingcomputer carries a caution about new ransom ware which denies a user access to his programs until a fee is paid because he/she is in violation of copyright law and must pay to clear the violation. There is always a need for vigilance. If you are being denied access to your lawful programs (as described), don't hesitate to seek assistance from the Club.

Kent Mullinex

kentm@bvres.org

Web sites to try

by Len

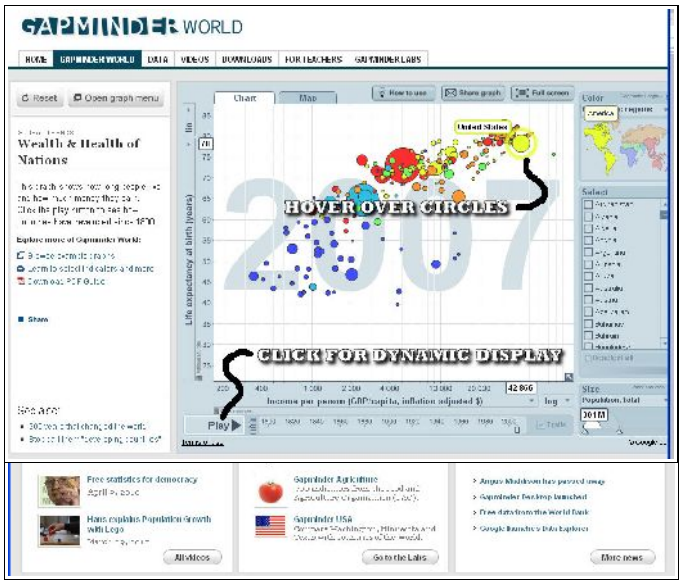
Dynamic Data

Here are some web sites to try during the BVCC summer vacation. The first one provides access to world statistics using interesting dynamic graphics presentation techniques.

http://www.gapminder.org/

The gapminder web site uses **Trendalyzer,** a new method of dynamically presenting data. No more static pie charts or bar graphs. **Trendalyzer** provides for dynamic interactive data presentation.

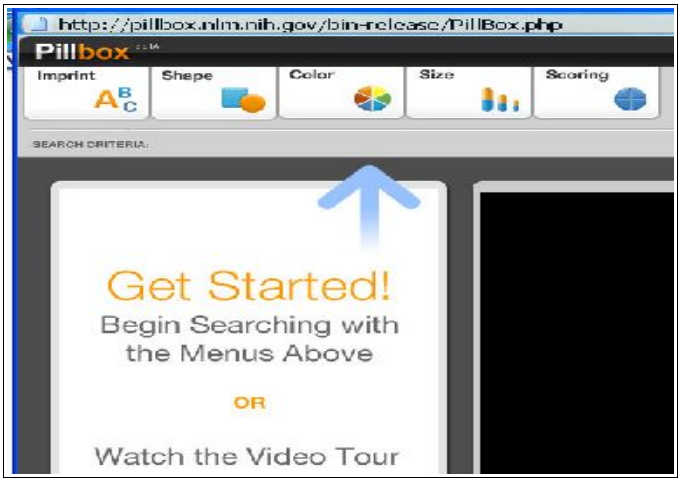
The following example shows wealth and health statistics. Countries and states are shown as circles, with the size of the circle related to population. The horizontal axis shows income per person and the vertical axis shows life expectancy in years.



If you hover the mouse pointer over a circle, the name of that area appears. If you click on the play button near the bottom of the display, a chart animation shows changes from 1800 to 2006.

There are other data sets available on the web site and there is also a 2 minute tutorial on how to use the site. Note that some of the databases take a little time to load.

What was that pill for?



Do you have any old pills that you are no longer sure what they are for? Here is a web site that can help.

http://pillbox.nlm.nih.gov/

> The National Library of Medicine is partnering with the Food and Drug Administration to enhance patient safety by providing an identification and reference system for solid-dosage medications.

This is apparently a work in progress. Since I do not have any old pills to identify I could not put it to a decent test. Perhaps some of our members might try out the web site and report back.

Search Engine for Weak Eyes?

A helpful programmer noticed that one of their relatives was having trouble seeing the entry boxes on Google and other search engines. So, **Good 50** was developed for those with vision issues.

http://good50.com/

Sounds like a good idea. However, after trying it out, I could not find any advantage over using Mozilla Firefox and pressing **Crtl +** [hold the **Ctrl** key down while pressing the **+** key] to enlarge the text on the display. **Ctrl-** reduces the text size.

BTW, the **Ctrl+** trick also works with the **Thunderbird** email program, and also works with **Internet Explorer** version **8**.

Zipcode Lookup

http://zip4.usps.com/zip4/

Need a zipcode for somewhere? The above link will take you to the USPS web site.

Future Stuff

Why not generate electricity from people's foot steps?

http://www.fastcompany.com/1617178/toulouse-france-tests-out-piezoelectric-pavement-power

More Useful Sites

Everyone has their own idea of useful. Here is a PC World Magazine writer's idea of useful sites.

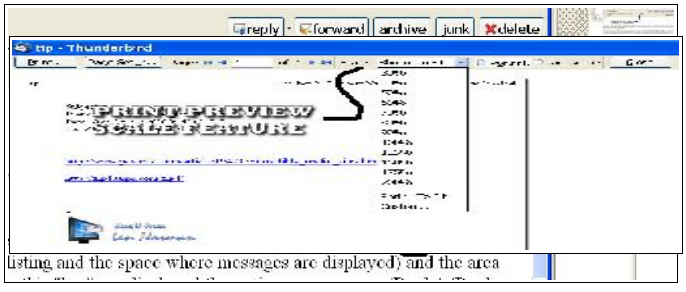
http://www.pcworld.com/article/194735/incredibly_useful_sites.html?tk=rss_news

Fred Notes

[Due to a hard drive crash, we had to install a new drive in Fred's computer. In the process, all of the programs had to be reinstalled. One of these was Thunderbird, the email program many BVCC members are using. Thunderbird recently released a new version (3.0.4) of the program and Fred noticed several new features. - Len]

Fred writes: In Thunderbird there is now a wide "toolbar" between the message list and the preview area where the message is displayed. On this "tool-bar" are displayed the options you can use **'Reply', 'Reply All', 'Forward', 'Delete**', etc. These are now more readily available.

The print command has been moved to a pop down menu on the new toolbar.



PRINT can also be be accessed through "**FILE**" Scroll down to "**PAGE SETUP**", or "**PRINT PRE-VIEW**" or "**PRINT**". **Page Setup** is used to change headers and margins . I like to use "**PRINT PREVIEW**". The copy appears. Tools on the top will open to % SCALE. You will find, reducing the % SCALE may reduce the number of sheets needed to print your copy - and still be legible !! Saving both paper and ink !! When finished printing, click on "**CLOSE**" to return to the message list. . ☺

Fred Schneiter

Virus warning:

by Len

Bogus Email

There is a new series of bogus email going around that include attachments that will make your computer sick. Here are a couple of examples:

> United Parcel Service of America.
>
> Dear customer!
>
> We failed to deliver the postal package sent on the 2nd of March in time because the addressee's address is not correct. Please print out the invoice copy attached and collect the package at our office.

> Dear customer!
>
> Unfortunately we were not able to deliver postal package which was sent on the 18th of February in time
>
> because the recipient's address is inexact.
>
> Please print out the invoice copy attached and collect the package at our office.
>
> DHL Global Services.

These messages have an attachment that has a zip file name extension. ***Never*** click on a file name with the extensions zip, exe, or pps unless you are 100% sure it is safe.

The other danger are emails that include links to Internet web sites. A recent example came disguised as email from the Bank of America. If you get any email requesting information about any kind of account, pick up the phone and call to verify if the message is real.

Antivirus Software

In the last couple of weeks we have had at least 3 BVCC members get attacked by a virus (see earlier article by Kent). It turns out that the antivirus software installed on there computers did not prevent the infection.

In one case, I spent several hours with a computer that had Norton installed and Norton not only did not prevent the virus, but it was worthless in getting rid of the virus.

A recent report notes problems created by the McAfee antivirus software.

http://www.computerworld.com/s/article/9175896/Flawed_McAfee_update_paralyzes_corporate_PCs?taxonomyId=125

Another virus, named Peachy, has been discovered attacking users of Adobe Acrobat. (Note: this does not apply to Acrobat Reader.)

Three points... First, I will not spend any more money for antivirus software. I will rely on ***Microsoft Security Essentials***.

Second, to make sure that loopholes in the Windows operating system and some Microsoft programs like Internet Explorer, the Windows update program should be used frequently to make sure the latest security patches are installed.

Third, no antivirus software will prevent someone from opening an infected attachment to an email, or from clicking on a web link. Practicing safe computing is the most effective way to prevent a computer from virus attacks.

More from Google

These days it seems that Google has unlimited funds to spend expanding their offerings and empire. By now I hope you have taken a look at Google Maps and used ***pegman*** to look at street views around the world (see the November 09 issue for a review of Google Maps).

Many of the Google offerings are free to users. Where does Google get all of that money you might ask.

Here is one example:

If you were looking to buy a new house, let's say in Waverly, OH, you could go to **Trulia.com** and search local listings. There are over 40,000 real estate companies in the US that are now using Trulia to list their offerings. And, Trulia programmers have written code that incorporates Google Maps (for a fee per use) into the home listings.

Here is another Google service.

If you have used Google Street views you know you can look at pictures of houses along an increasing number of streets. Now Google is offering business the opportunity to invite Google photographers right into the company. Soon, you can walk down a street in Google Maps, look at a store front, and then walk right into the store.

What will they think of next?

See You in the Fall